

EXPRESS MAIL CERTIFICATE

Date 8/8/01 Label No. EL 903057264-45

I hereby certify that, on the date indicated above, this paper or fee was deposited with the U.S. Postal Service & that it was addressed for delivery to the Assistant Commissioner for Patents, Washington, DC 20231 by "Express Mail Post Office to Addressee" service.

B.W. LEE B.W. Lee
Name (Print) Signature



PLEASE CHARGE ANY DEFICIENCY UP TO \$300.00 OR CREDIT ANY EXCESS IN THE FEES DUE WITH THIS DOCUMENT TO OUR DEPOSIT ACCOUNT NO. 04-0100

Customer No.:



07278

PATENT TRADEMARK OFFICE

Docket No.: 6727/OJ351USO

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Dror, Itai et al.

Serial No.: 09/854,853

Filed: May 14, 2001

For: EXTENDING THE RANGE OF COMPUTATIONAL FIELDS OF INTEGERS

August 8, 2001

INFORMATION DISCLOSURE STATEMENT

Hon. Commissioner of
Patents and Trademarks
Washington, DC 20231

Sir:

This Information Disclosure Statement is submitted in accordance with 37 C.F.R. 1.97, 1.98, and it is requested that the information set forth in this statement and in the listed documents be considered during the pendency of the above-identified application, and any other application relying on the filing date of the

above-identified application or cross-referencing it as a related application.

1. This IDS should be considered, in accordance with 37 C.F.R. 1.97, as it is filed: (Check one of the boxes A-D)

☒ A. Within three months of the filing date of the above-identified national application or within three months of the entry into the national stage of the above-identified international application.

☐ B. before the mailing date of a first office action on the merits, or a first office action after filing a request for continued examination.

☐ C. after (A) and (B) above, but before the mailing date of a final rejection, a notice of allowance, or any other action that closes prosecution, and Applicants have made the necessary statement in box "i" below or paid the necessary fee in box "ii" below.

(check one of the boxes "i" and "ii" below:)

☐ i. Counsel states that, upon information and belief, each item of information listed herein was either (a) cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this IDS; or (b) was not cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of undersigned after making reasonable inquiry, was not known to any individual designated in 1.56(c) more than three months prior to the filing of this IDS.

☐ ii. A check for the fee set forth in 1. 17(p), presently believed to be \$180, is enclosed.

☐ D. after (A), (B) and (C) above, but before payment of the issue fee: Counsel states that, upon information and belief, each item of information listed herein was either (i) cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the IDS; or (ii) was not cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of the undersigned after making reasonable inquiry, was not known to any individual designated in 1.56(c) more than three months prior to the filing of this IDS.

☐ i. A check for the fee set forth in 1.17 (p), presently believed to be \$180, is enclosed.

2. In accordance with 37 C.F.R. 1.98, this IDS includes a list (e.g., form PTO-

Docket No.6727/0J351US0

1449) of all patents, publications, or other information submitted for consideration by the office, either incorporated into this IDS or as an attachment hereto. A copy of each document listed is attached, except as explained below.

(check boxes A and/or B and fill in blanks, if appropriate.)

- ☐ A. Document(s) _____ is (are) deemed substantially cumulative to document(s) _____, and, in accordance with 1.98(c), only a copy of each of the latter documents is enclosed.
- ☐ B. Certain documents were previously cited by or submitted to the Office in the following prior applications, which are relied upon under 35 U.S.C. 120:

[SERIAL NO. & FILING DATE].

Applicant Identifies these documents by attaching hereto copies of the forms PTO-892 and PTO- 1449 from the files of the prior application(s) or a fresh PTO- 1449 listing these documents, and request that they be considered and made of record in accordance with 1.98(d). Per 37 CFR 1.98(d), copies of these documents need not be filed in this application.

☐ 3. Document(s) _____ are not in the English language. In accordance with 1.98(c), Applicant states:

- ☐ An English translation of each document (or of the pertinent portions thereof), or a copy of each corresponding English-language patent or application is enclosed.
- ☐ A concise explanation of the relevance of document(s) _____ is found in the attached search report (see MPEP § 609 A(3)x).
- ☐ A concise explanation of the relevance of document(s) _____ is set forth as follows: [Insert concise explanation of relevance]
- ☐ A concise explanation of the relevance of document(s) _____ can be found on page(s) _____ of the specification.

Docket No.6727/0J351US0

☐ A concise explanation of document(s) _____ can be found on the attached sheet.

☐ 4. No explanation of relevance is necessary for documents in the English language (see MPEP § 609 A(3)).

☐ 5. Other information being provided for the examiner's consideration follows:

6. In accordance with 37 C.F.R. 1.97(g) and (h), the filing of this IDS should not be construed as a representation that a search has been made or that information cited is, or is considered to be, material to patentability as defined in § 1.56 (b), or that any cited document listed or attached is (or constitutes) prior art. Unless otherwise indicated, the date of publication indicated for an item is taken from the face of the item and Applicant reserves the right to prove that the date of publication is in fact different.

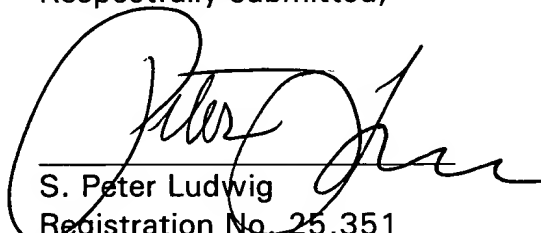
CROSS REFERENCE UNDER 37 C.F.R. § 1.78 TO RELATED APPLICATIONS

Pursuant to 37 C.F.R. § 1.79, Applicant notes that the above-identified patent application may be related to the following U.S. Patent Applications:

(1) U.S. Patent Application Serial No _____, filed _____.

Early and favorable consideration is earnestly solicited.

Respectfully submitted,


S. Peter Ludwig
Registration No. 25,351
Attorney for Applicant(s)

DARBY & DARBY P.C.
805 Third Avenue
New York, N.Y. 10022
(212) 527-7700



FORM PTO-1449 (Colb)	ATTY DOCKET NUMBER 6727/0J351US0	SERIAL NUMBER 09/854,853
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANTS' INFORMATION STATEMENT	APPLICANT Itai DROR, et al.	
	FILING DATE May 14, 2001	GROUP ART UNIT 2131

U.S. PATENT DOCUMENTS

Examiner's Initials		DOCUMENT NO.	DATE	NAME	CLASS	SUB	FILING DATE
	AA	5,742,530	4/21/98	Gressel et al.	364	746	12/28/95
	AB	5,513,133	4/30/96	Cressel et al.	364	754	11/18/93
	AC	5,448,639	9/5/95	Arazi	380	30	4/13/93
	AD	5,261,001	11/9/93	Dariel et al.	380	30	3/2/92
	AE	5,206,824	4/27/93	Arazi	364	746.1	5/17/91
	AF	4,745,568	5/17/88	Onyszchuk et al.	364	754	5/30/85
	AG	4,587,627	5/6/86	Omura et al.	364	754	11/14/82
	AH						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB	TRANS- LATION
	AI	WO 98/50851	Nov. 1998	PCT	G06F	7/37	Yes

OTHER ART (Including Author, Bills, Pertinent Pages, Etc.)

	AJ	C. Parr et al., "Fast Arithmetic for Public-Key Algorithms in Galois fields with Composite Exponents", <i>IEEE Transactions on Computers</i> , Vol. 48, No. 10, Oct. 1999.
	AK	W. Wesley Peterson et al., <u>Error-Correcting Codes</u> , 2 nd Edition, MIT Press, Cambridge, MA, 1972, pp. 174-179.
	AL	Lecture by Marco Bucci of the Fondazione Ugo Bordoni, Eurocrypt Conference Rump Session, Perugia, Italy, 1994.

EXAMINER:	DATE CONSIDERED:
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

FORM PTO-1449 (Colb)	ATTY DOCKET NO. 6727/0J351US0	SERIAL NUMBER 09/854,853
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANTS' INFORMATION STATEMENT	APPLICANT Itai DROR, et al.	
	FILING DATE May 14, 2001	GROUP ART UNIT 2131

U.S. PATENT DOCUMENTS

Examiner's Initials		DOCUMENT NO.	DATE	NAME	CLASS	SUB	FILING DATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB	TRANS- LATION
	AI						
	AJ						
	AK						

OTHER ART (Including Author, Bills, Pertinent Pages, Etc.)

AL	The ST19-CF58 Device, produced by STMicroelectronics, Rousset, France.
AM	D. Knuth, <u>The Art of Computer Programming, Vol. 2: Seminumerical Algorithms</u> , Addison-Wesley, Reading, MA, 1981.
EXAMINER: _____ DATE CONSIDERED: _____	
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	